

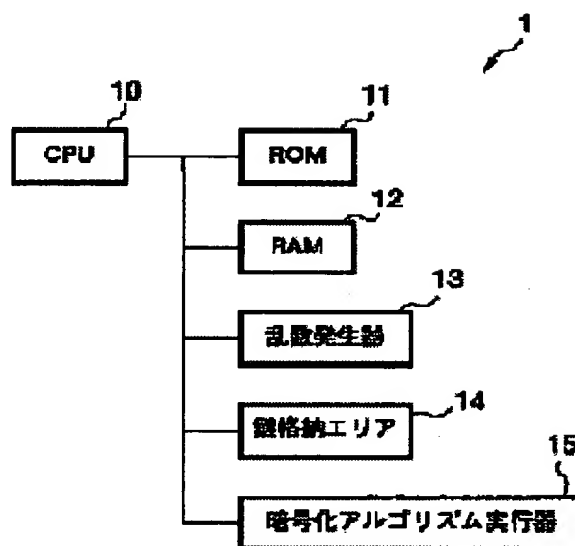
SYSTEM AND METHOD FOR TOLL COLLECTION

Patent number: JP10134214
Publication date: 1998-05-22
Inventor: NAITO KAZUTOSHI; FUKAZAWA KAZUO; KAWAMURA SHINICHI; KITAORI MASASHI
Applicant: TOSHIBA CORP
Classification:
- **international:** G07B15/00; G07B15/00; G06K17/00; G08G1/017; H04L9/32
- **european:**
Application number: JP19960290616 19961031
Priority number(s):

Abstract of JP10134214

PROBLEM TO BE SOLVED: To improve the security of a radio communication line of the toll reception system which receives a toll by radio.

SOLUTION: The CPU 10 of an IC card 1 inserted into an OBU(on-board unit) receives a cipher key sent from a roadside system and a authenticator generated by ciphering algorithm through OBU, deciphers the authenticator with a cipher key stored previously in a key storage area 14 to confirm the adequacy of the roadside system, and issues an authenticator by a ciphering algorithm execution unit 15 with the cipher key stored in the key storage area 14 when the key is proper and sends it to the roadside system through OBU, and the roadside system deciphers the received authenticator to confirm the adequacy of the IC card 1, and totalizes toll information when the key is proper.



Data supplied from the *esp@cenet* database - Worldwide

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-134214

(43) 公開日 平成10年(1998) 5月22日

(51) Int.Cl. ⁶	識別記号	F I	
G 0 7 B 15/00		G 0 7 B 15/00	J
			L
	5 1 0		5 1 0
G 0 6 K 17/00		G 0 6 K 17/00	L
G 0 8 G 1/017		G 0 8 G 1/017	
審査請求 未請求 請求項の数 9 O L (全 12 頁) 最終頁に続く			

(21) 出願番号 特願平8-290616

(22) 出願日 平成 8 年 (1996) 10 月 31 日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 内藤 一敏

東京都港区芝浦一丁目1番1号 株式会社

東芝本社事務所内

(72) 発明者 深沢 一夫

神奈川県川崎市幸区柳町70番地 株式会社

東芝柳町工場内

(72) 発明者 川村 信一

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

(74) 代理人 弁理士 鈴江 武彦 (外6名)

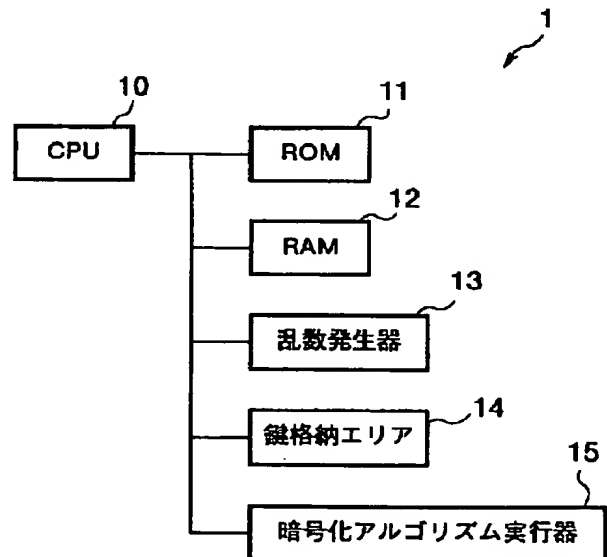
最終頁に続く

(54) 【発明の名称】 料金収受システムと料金収受方法

(57) 【要約】

【課題】 無線で料金の収受を行なう料金収受システムにおける無線通信回線のセキュリティの向上を図る。

【解決手段】 OBUに挿入されたICカード1のCPU 10は、路側システムから送信される暗号鍵と暗号化アルゴリズムで発生された認証子をOBUを介して受信し、この認証子を鍵格納エリア14に予め格納した暗号鍵で復号化して上記路側システムの正当性を確認し、鍵が正当な場合に鍵格納エリア14に格納した暗号鍵と暗号化アルゴリズム実行器15により認証子を発行し、OBUを介して路側システムへ送信し、路側システムで受信された認証子が復号化されてICカード1の正当性が確認され、鍵が正当な場合に課金情報として集計される。



【特許請求の範囲】

【請求項1】 車両に設けられ、ＩＣカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受システムにおいて、

上記車内装置は、

上記ＩＣカードに対して暗号鍵を用いた情報を送信する送信手段と、

この送信手段による送信に基づいた上記ＩＣカードからの応答を受信する受信手段と、

この受信手段による受信に基づいて上記ＩＣカードの正当性が確認された場合に第１の方式、正当性が確認されない場合に第２の方式にて上記ＩＣカードの処理を行う制御手段と、

を具備したことを特徴とする料金収受システム。

【請求項2】 車両に設けられ、ＩＣカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受システムにおいて、

上記車内装置は、

上記ＩＣカードに対して暗号鍵を用いた情報を送信する送信手段と、

この送信手段による送信に基づいた上記ＩＣカードからの応答を受信する受信手段と、

この受信手段にて上記ＩＣカードより応答を受信したとき第１の方式、応答を受信できないとき上記第１の方式とは異なる第２の方式で上記ＩＣカードの処理を行う制御手段と、

を具備したことを特徴とする料金収受システム。

【請求項3】 車両に設けられ、ＩＣカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受システムにおいて、

上記車内装置は、

挿入されるＩＣカードに対して暗号鍵を用いた情報を送信する送信手段と、

この送信手段による送信に基づいた上記ＩＣカードからの応答を受信する受信手段と、

この受信手段による受信に基づいて上記ＩＣカードの正当性が確認された場合に第１の方式、正当性が確認されない場合に第２の方式に切り換える切換手段と、
を具備したことを特徴とする料金収受システム。

【請求項4】 車両に設けられ、ＩＣカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受システムにおいて、

上記車内装置に挿入されたＩＣカードが、

上記車内装置から送信される暗号鍵を用いた情報を受信する受信手段と、

この受信手段で受信された情報から予め格納された暗号

鍵を用いて上記車内装置の正当性を確認する第１の確認手段と、

上記第１の確認手段で正当性が確認された場合、上記予め格納された暗号鍵を用いた情報を発行する発行手段と、

この発行手段で発行された情報を上記車内装置に送信する送信手段と、

上記車内装置が、

上記送信手段で送信された情報から予め格納された暗号鍵を用いて上記ＩＣカードの正当性を確認する第２の確認手段と、

この第２の確認手段で上記ＩＣカードの正当性が確認されなかった場合、上記ＩＣカードを返却する返却手段と、

上記第２の確認手段で上記ＩＣカードの正当性が確認された場合、上記ＩＣカードを認証して上記路側システムと無線によって料金収受の制御を行う制御手段と、
を具備したことを特徴とする料金収受システム。

【請求項5】 車両に設けられ、ＩＣカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受システムにおいて、

上記車内装置に挿入されたＩＣカードが、

上記車内装置から送信される暗号鍵を用いた情報を受信する第１の受信手段と、

この第１の受信手段で受信された情報を予め格納された暗号鍵を用いて上記車内装置の正当性を確認する第１の確認手段と、

この第１の確認手段で正当性が確認された場合、上記予め格納された暗号鍵を用いて情報を発行する発行手段と、

この発行手段で発行された情報を上記車内装置に送信する送信手段と、

上記車内装置が、上記送信手段で送信された情報を受信する第２の受信手段と、

この第２の受信手段で受信された情報を予め格納された暗号鍵を用いて上記

ＩＣカードの正当性を確認する第２の確認手段と、この第２の確認手段で正当性が確認された場合のみ上記路側システムと無線によって料金収受の制御を行う制御手段と、

を具備したことを特徴とする料金収受システム。

【請求項6】 車両に設けられ、ＩＣカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受方法であって、

上記車内装置が、上記ＩＣカードに対して暗号鍵を用いた情報を送信し、この送信に基づいた上記ＩＣカードからの応答を受信し、上記ＩＣカードより応答を受信したとき第１の方式、応答を受信できないとき上記第１の方

式とは異なる第2の方式で上記ICカードの処理を行うようにしたことを特徴とする料金収受システム。

【請求項7】 車両に設けられ、ICカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受方法であって、

上記車内装置と挿入されるICカードとの間で暗号鍵を用いて正当性を確認し、正当性が確認された場合に第1の方式、正当性が確認されない場合に第2の方式に切り換えて上記車内装置が上記路側システムと無線によって料金収受を行うようにしたことを特徴とする料金収受方法。

【請求項8】 車両に設けられ、ICカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受方法であって、

上記車内装置と挿入されるICカードとの間で暗号鍵を用いて正当性を確認し、正当性が確認された場合に上記車内装置と上記路側システムとの間で無線によって料金収受を行い、正当性が確認されない場合に上記車内装置に挿入されたICカードと上記路側システムとの間で暗号鍵を用いて正当性を確認し、正当性が確認された場合に料金収受を行うようにしたことを特徴とする料金収受方法。

【請求項9】 車両に設けられ、ICカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受方法であって、

上記車内装置と挿入されるICカードとの間で暗号鍵を用いてICカードの正当性を確認し、ICカードの正当性が確認された場合のみ上記車内装置と上記路側システムとの間で無線によって料金収受を行うようにしたことを特徴とする料金収受方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、例えば有料道路において、車両等の移動体に搭載されている車載機器と無線によって料金収受を行う料金収受システムと料金収受方法に関する。

【0002】

【従来の技術】 従来、例えば有料道路における料金収受装置の端末装置を備える料金所において、有料道路本線に入線する車両に対して料金所の入口の端末装置で入口情報（料金所の識別番号、車種、時刻等）を記録した通行券を発行し、上記料金所と有料道路で接続されている他の料金所の出口で、上記料金所で発行された通行券の入口情報により、この料金所の出口に備えられている端末装置を用いて通行料金を計算し、通行料金の収受を行っている。

【0003】 この料金収受装置は、複数の端末装置を持

って各料金所に設置されている。料金所の入口の各端末装置は、有料道路本線に入線する車両に対して入口情報（料金所の識別番号、車種、時刻等）を記録した通行券を発行する。料金所の出口の各端末装置は、通行料金計算のためのテーブル、例えば全ての料金所との区間料金、車種別の料金等をメモリに記憶しており、料金所の出口において料金所の入口で発行された通行券の入口情報によりメモリに記憶している通行料金テーブルを検索して通行料金を計算する。

10 【0004】 それに対して、車両に搭載した車載機器と地上（料金所）側の通信装置と無線で料金の収受を行う料金収受システムが、非接触、ノンストップのメリットをユーザに提供する手段として注目を受けている。

【0005】 しかしながら、このような無線で料金の収受を行なう料金収受システムにおいては、無線通信回線のセキュリティに関する検討が不足している。そのため、無線通信回線上のセキュリティに課題があり、改竄・偽造が発生する恐れがある。

【0006】

20 【発明が解決しようとする課題】 上記したように、無線で料金の収受を行なう料金収受システムにおいては、無線通信回線のセキュリティに関する検討が不足している。そのため、無線通信回線上のセキュリティに課題があり、改竄・偽造が発生する恐れがあるという問題があった。

【0007】 そこで、この発明は、無線で料金の収受を行なう料金収受システムにおける無線通信回線のセキュリティの向上を図ることのできる料金収受システムと料金収受方法を提供することを目的とする。

30 【0008】

【課題を解決するための手段】 この発明の料金収受システムは、車両に設けられ、ICカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受システムにおいて、上記車内装置は、上記ICカードに対して暗号鍵を用いた情報を送信する送信手段と、この送信手段による送信に基づいた上記ICカードからの応答を受信する受信手段と、この受信手段による受信に基づいて上記ICカードの正当性が確認された場合に第1の方式、正当性が確認されない場合に第2の方式にて上記ICカードの処理を行う制御手段とから構成されている。

40 【0009】 この発明の料金収受システムは、車両に設けられ、ICカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受システムにおいて、上記車内装置は、上記ICカードに対して暗号鍵を用いた情報を送信する送信手段と、この送信手段による送信に基づいた上記ICカードからの応答を受信する受信手段と、この受信手段にて上記ICカードより応答を受信したとき第1の方式、応答を受信できないとき上記第1の

方式とは異なる第2の方式で上記ICカードの処理を行う制御手段とから構成されている。

【0010】この発明の料金収受システムは、車両に設けられ、ICカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受システムにおいて、上記車内装置は、挿入されるICカードに対して暗号鍵を用いた情報を送信する送信手段と、この送信手段による送信に基づいた上記ICカードからの応答を受信する受信手段と、この受信手段による受信に基づいて上記ICカードの正当性が確認された場合に第1の方式、正当性が確認されない場合に第2の方式に切り換える切換手段とから構成されている。

【0011】この発明の料金収受システムは、車両に設けられ、ICカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受システムにおいて、上記車内装置に挿入されたICカードが、上記車内装置から送信される暗号鍵を用いた情報を受信する受信手段と、この受信手段で受信された情報から予め格納された暗号鍵を用いて上記車内装置の正当性を確認する第1の確認手段と、上記第1の確認手段で正当性が確認された場合、上記予め格納された暗号鍵を用いた情報を発行する発行手段と、この発行手段で発行された情報を上記車内装置に送信する送信手段と、上記車内装置が、上記送信手段で送信された情報から予め格納された暗号鍵を用いて上記ICカードの正当性を確認する第2の確認手段と、この第2の確認手段で上記ICカードの正当性が確認されなかった場合、上記ICカードを返却する返却手段と、上記第2の確認手段で上記ICカードの正当性が確認された場合、上記ICカードを認証して上記路側システムと無線によって料金収受の制御を行う制御手段とから構成されている。

【0012】この発明の料金収受システムは、車両に設けられ、ICカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受システムにおいて、上記車内装置に挿入されたICカードが、上記車内装置から送信される暗号鍵を用いた情報を受信する第1の受信手段と、この第1の受信手段で受信された情報を予め格納された暗号鍵を用いて上記車内装置の正当性を確認する第1の確認手段と、この第1の確認手段で正当性が確認された場合、上記予め格納された暗号鍵を用いて情報を発行する発行手段と、この発行手段で発行された情報を上記車内装置に送信する送信手段と、上記車内装置が、上記送信手段で送信された情報を受信する第2の受信手段と、この第2の受信手段で受信された情報を予め格納された暗号鍵を用いて上記ICカードの正当性を確認する第2の確認手段と、この第2の確認手段で正当性が確認された場合のみ上記路側システムと無線によって料金

収受の制御を行う制御手段とから構成されている。

【0013】この発明の料金収受方法は、車両に設けられ、ICカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受方法であって、上記車内装置が、上記ICカードに対して暗号鍵を用いた情報を送信し、この送信に基づいた上記ICカードからの応答を受信し、上記ICカードより応答を受信したとき第1の方式、応答を受信できないとき上記第1の方式とは異なる第2の方式で上記ICカードの処理を行うようにしたことを特徴とする。

【0014】この発明の料金収受方法は、車両に設けられ、ICカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受方法であって、上記車内装置と挿入されるICカードとの間で暗号鍵を用いて正当性を確認し、正当性が確認された場合に第1の方式、正当性が確認されない場合に第2の方式に切り換えて上記車内装置が上記路側システムと無線によって料金収受を行うようにしたことを特徴とする。

【0015】この発明の料金収受方法は、車両に設けられ、ICカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受方法であって、上記車内装置と挿入されるICカードとの間で暗号鍵を用いて正当性を確認し、正当性が確認された場合に上記車内装置と上記路側システムとの間で無線によって料金収受を行い、正当性が確認されない場合に上記車内装置に挿入されたICカードと上記路側システムとの間で暗号鍵を用いて正当性を確認し、正当性が確認された場合に料金収受を行うようにしたことを特徴とする。

【0016】この発明の料金収受方法は、車両に設けられ、ICカードが挿入される車内装置と、この車内装置と情報の通信を行う路側システムとから構成され、車両の料金収受を行う料金収受方法であって、上記車内装置と挿入されるICカードとの間で暗号鍵を用いてICカードの正当性を確認し、ICカードの正当性が確認された場合のみ上記車内装置と上記路側システムとの間で無線によって料金収受を行うようにしたことを特徴とする。

【0017】

【発明の実施の形態】以下、この発明の一実施例について図面を参照して説明する。この発明に関わる料金収受システムは、入口車線及び出口車線から構成される入口発券出口収受方式（以下、クローズドシステムと記述する）と、均一車線のみで構成されるオープンシステムとに分けられる。

【0018】また、詳しくは後述するが車両に搭載される車載機器は、無線通信機能や操作部、表示部を備えた車内装置としてのオンボードユニット（On Board Unit

：以下、OBUと記述する）2と利用者のID番号・口座番号（以下、課金情報と記述する）を備えたICカード1とから構成されている。

【0019】また、OBU2には、予め搭載する車両の車種を決定する要因の長さ・軸数・重量・用途・特長のデータ（以下、車両情報と記述する）が登録されている。ICカード1には、課金情報が記憶されている。

【0020】図1は、この発明の料金収受システムに係るICカード1の構成を示すものである。すなわち、ICカード1は、全体の制御を司るCPU10、制御プログラム等を記憶しているROM11、課金情報等を記憶するRAM12、乱数を発生する乱数発生器13、後述するセキュリティ方式Aまたはセキュリティ方式Bのための鍵が格納される鍵格納エリア14、及び暗号化アルゴリズム実行器15とから構成されている。

【0021】図2は、OBU2の構成を示すものである。すなわち、OBU2は、全体の制御を司るCPU20、制御プログラム等を記憶しているROM21、車両情報等を記憶するRAM22、乱数を発生する乱数発生器23、後述するセキュリティ方式Bのための鍵が格納される鍵格納エリア14、暗号化アルゴリズム実行器15、各車線に設置されたアンテナと交信を行うアンテナ26、アンテナ26の制御を行う無線通信制御部27、操作案内をする文字表示とLEDランプを備えた表示部28、複数のボタンを備えた操作部29、及びICカード1が装着されて読取り・書込みが可能なICカード処理部18とから構成されている。

【0022】図3は、クローズドシステムに用いられる入口車線機器の構成を示すものである。すなわち、入口車線機器は、車両の進行方向から車種判別装置31、第1アンテナ32、通行券自動発行機30、発進検知装置33、及び第2アンテナ34とから構成されている。

【0023】車種判別装置31は、進入した車両を検知し、車両の進入を通行券自動発行機30に伝達する。さらに、進入した車両の車種を判別し、判定結果を通行券自動発行機30に通知する。

【0024】第1アンテナ32は、通行券自動発行機30の指示により、進入した車両に搭載された車載機器との通信を行うものである。発進検知装置33は、車両の発進を検知し、通行券自動発行機30に通知する。

【0025】第2アンテナ34は、第1アンテナ32で正常に交信が終了した車両が発進検知装置33に進入することにより、通行券自動発行機30の指示の元で、車載機器との通信を行うものである。

【0026】通行券自動発行機30は、各機器の制御を行うと同時に、車載機器を搭載していない車両（以下、非ETC車と記述する）に対して通行券を発行する。通行券自動発行機30にはネガティブリストが登録されている。

【0027】図4は、クローズドシステムに用いられる

出口車線機器の構成を示すものである。図4の（a）に示すように出口車線機器は、車両の進行方向から車両検知装置41、第1アンテナ42、出口ブース内機器43、車両検知装置44、及び第2アンテナ45とから構成されている。

【0028】出口ブース内機器43は、図4の（b）に示すように非ETC車が持参した通行券を処理する通行券確認機46、前納のカードを処理するカード処理機47、現金支払い車に対する領収書発行を行う領収書発行機48、各機器の制御を行う出口車線制御装置40とから構成されている。出口車線制御装置40は、ネガティブリストが登録されている。なお、通行券確認機46は、ICカード1を処理することのできるICカードリーダー46aを備えている。

【0029】車両検知装置41は、車両の進入を検知した結果を出口ブース内機器43の出口車線制御装置40に通知する。第1アンテナ42は、出口車線制御装置40の制御の元で、進入車両に搭載された車載機器との交信を行うものである。

【0030】車両検知装置44は、車両の進入を検知した結果を出口車線制御装置40に通知する。第2アンテナ45では、出口車線制御装置40の制御の元で、車両に搭載された車載機器との交信を行う。

【0031】図5は、オープンシステムに用いられる均一車線機器の構成を示すものである。図5の（a）に示すように均一車線機器は、車両の進行方向から車両検知装置51、第1アンテナ52、ブース内機器53、車両検知装置54、及び第2アンテナ55とから構成されている。

【0032】ブース内機器53は、図5の（b）に示すように料金支払種別や進入車両の車種を入力し、各機器の制御を行う料金処理機50、前納のカードを処理するカード処理機56、現金支払い車に対する領収書の発行を行う領収書発行機57、ICカード1を処理することのできるICカードリーダー58とから構成されている。なお、料金処理機50にはネガティブリストが登録されている。

【0033】車両検知装置51は、車両の進入を検知した結果をブース内機器53の料金処理機50に通知する。第1アンテナ52は、料金処理機50の制御の元で、進入車両に搭載された車載機器との交信を行うものである。

【0034】車両検知装置54は、車両の進入を検知した結果を料金処理機50に通知する。第2アンテナ55では、料金処理機50の制御の元で、車両に搭載された車載機器との交信を行う。

【0035】車線側の機器を総称して以下、路側システムと記述する。利用者は、車両に車載機器を搭載し、OBU2にICカード1を挿入した状態で走行する。OBU2に挿入されたICカード1は、OBU2の正当性を

確認することにより、OBU2に対してカードID番号を通知する。

【0036】次に、クローズシステムの道路を利用する例について説明する。入口車線では、車種判別装置31が車両の進入を検知することにより、通行券自動発行機30に進入検知を伝達する。通行券自動発行機30は、第1アンテナ32を制御し、進入する車両に搭載されている車載機器（ICカード1が挿入されたOBU2）に対する交信問い合わせを開始する。車載機器は、正当なアンテナからの問い合わせと認識することにより、予めICカード1から通知されたID番号とOBU2に記録されている車両情報を返信する。

【0037】通行券自動発行機30は、車載機器からの応答が正当と認識することにより、ICカード1のID番号をネガティブリストと照合し、正当であれば入口を特定する道路番号・料金所番号・通過年月日時分・車線番号（以下、入口情報Aと記述する）を車載機器に送信する。OBU2では、入口情報Aの受信が正常に行われたことを確認して、路側システムに受信完了を通知する。

【0038】路側システムは、車載機器からの受信完了を受けることにより、通行券自動発行機30に発券停止を指示し、正常な車載機器搭載車両（以下、ETC車と記述する）と認定する。

【0039】ETC車が発信検知装置33を通過することにより、通行券自動発行機30は、発信検知装置33から車両進入の通知を受け、第2アンテナ34を制御し、車載機器に対する交信問い合わせを実行する。車載機器は、正当なアンテナからの問い合わせと認識することにより、予めICカード1から通知されたID番号を通知する。

【0040】通行券自動発行機30は、車載機器からの応答が正当と認識することにより、ICカード1のID番号を第1のアンテナ32で受信したものと比較し、一致していれば車種判別装置31から受信した車種判定結果を入口情報Bとして第2アンテナ34を利用して車載機器に返信する。

【0041】車載機器（ICカード1が挿入されたOBU2）では、入口情報Bのデータが正常に受信されたことを確認し、第2アンテナ34に受信完了を通知する。同時に車載機器では、正常に受信した入口情報Aと入口情報BとをICカード1に入口情報（入口情報Aと入口情報Bとを合わせたものを入口情報とする）として記録する。

【0042】出口車線では、車両検知装置41が車両の進入を検知することにより、車両の進入を出口車線制御装置40に通知する。出口車線制御装置40では、第1アンテナ42を制御し、進入した車両に対して問い合わせを実行する。出口車線でも入口車線同様に相手の正当性を認識することにより、車載機器は、OBU2に記録

されている入口情報及び課金情報を第1アンテナ42に伝送する。

【0043】出口車線制御装置40では、第1アンテナ42を経由して受信した入口情報を元に通行料金の算出を行い、同時にID番号のネガティブリスト照合を行い、ID番号の正当性を認識することにより、入口情報及び出口情報（料金所番号・通過年月日時分・車線番号・通行料金）を利用履歴として、OBU2に伝送する。OBU2では、利用履歴が正常に受信完了したことを確認し、路側システムに受信完了を通知する。同時に、ICカード1に対して利用履歴を記録する。

【0044】次に、オープンシステムの均一車線について説明する。上述したクローズシステムと同様に利用者は、車両に車載機器を搭載し、OBU2にICカード1を挿入した状態で走行する。ICカード1は、OBU2の正当性確認を行い、ID番号を通知しておく。

【0045】均一車線では、車両検知装置51が車両の進入を検知することにより、料金処理機50に車両進入を通知する。料金処理機50は、第1アンテナ52を制御し、車載機器に対して問い合わせを実行する。上述した入口車線と同様に相手の正当性を認識することにより、OBU2は、予め通知されたICカード1のID番号とOBU2に記録された車両情報を第1アンテナ52に送信する。

【0046】料金処理機50では、第1アンテナ52を経由して受信したID番号をネガティブリストと照合し、正当性が認識された場合、車両情報を元にした車種判定が行われ、判定した車種で通行料金を算出する。算出結果を元に料金所情報（料金所番号・通過年月日時分・車線番号・通行料金）を生成し、利用履歴としてOBU2に伝送する。

【0047】OBU2では、利用履歴が正常に受信完了したことを確認し、路側システムに受信完了を通知する。同時に、ICカード1に対して、利用履歴を記録する。図6は、この発明に係る通行券自動発行機30の構成を示すものである。すなわち、通行券自動発行機30は、各機器と接続されて全体の制御を司るCPU301、制御プログラム等を記憶しているROM302、各種情報を記憶するRAM303、乱数を発生する乱数発生器304、後述するセキュリティ方式Aのための鍵が格納される鍵格納エリア305、暗号化アルゴリズム実行器306、及び通行券発行処理部307とから構成されている。

【0048】図7は、この発明に係る出口車線制御装置40の構成を示すものである。すなわち、出口車線制御装置40は、各機器と接続されて全体の制御を司るCPU401、制御プログラム等を記憶しているROM402、各種情報を記憶するRAM403、乱数を発生する乱数発生器404、後述するセキュリティ方式Aのための鍵が格納される鍵格納エリア405、及び暗号化アル

ゴリズム実行器406とから構成されている。

【0049】次に、このような構成において、本発明に係る入口発券出口収受方式（クロズドシステム）におけるセキュリティシステムについて説明する。ここでは、鍵の受け渡しに関する概念を記述する。

【0050】まず、セキュリティ方式Aを図8のフローチャートを参照して説明する。OBU2にICカード（ICC）1が挿入された車載機器を搭載した車両が通過する路側システム（RSE）の入口車線において、通行券自動発行機30のCPU301は、鍵格納エリア305に格納している暗号鍵（秘密鍵あるいは公開鍵）Kを用いて、乱数発生器304により発生させた乱数を暗号化アルゴリズム実行器306で暗号化させて認証子K_rを発行し、通過する車両に搭載された車載機器のOBU2に対して送信する。

【0051】OBU2は、受信した認証子K_rをそのまま挿入されているICカード1に対して送信する。ICカード1のCPU10は、受信した認証子K_rを鍵格納エリア14に格納している暗号鍵（秘密鍵あるいは公開鍵）Kで復号化し、路側システムの正当性を確認する。もし、鍵が正当でなかった場合（処理NG）、路側システムの出口車線で車両は停止される。

【0052】CPU10は、鍵が正当と確認された場合、認証子K_rに鍵格納エリア14に格納している暗号鍵Kと暗号化アルゴリズム実行器15を用いて認証子K_r+K_iを発行してOBU2へ送信する。

【0053】なお、路側システムとOBU2との間のデータ伝送は高速化されているが、OBU2とICカード1の間は伝送速度が遅く（数秒単位）、入口車線通過時間（ms単位）内に処理を完了させるのは難しい状況である。従って、OBU2とICカード1との間のデータ伝送に関する処理時間は入口車線から出口車線までの間の車両走行中に実施するようになっている。

【0054】上記車両が通過する路側システムの出口車線において、OBU2に予め伝送されている認証子K_r+K_iが路側システムの出口車線に送信される。出口車線制御装置40のCPU401は、受信した認証子K_r+K_iを鍵格納エリア14に格納している暗号鍵Kで復号化してICカード1の正当性を確認する。もし、鍵が正当でなかった場合（処理NG）、路側システムの出口車線で車両を停止する。

【0055】CPU401は、鍵が正当と確認された場合に課金情報として集計する。次に、セキュリティ方式Bを図9のフローチャートを参照して説明する。このセキュリティ方式Bは、車両が料金所進入前に、事前にOBU2に対してデータ送信が可能な方式である。

【0056】車両に搭載された車載機器のOBU2にICカード1が挿入された際、OBU2は挿入されたICカード1とのデータ送受信を開始するが、データ送受信を行う前にセキュリティ上の相互認証を行う必要があ

る。

【0057】まず、OBU2のCPU20は、乱数発生器23で乱数を発生させ、鍵格納エリア24に格納された暗号鍵を用いて暗号化アルゴリズム実行器25で暗号化させて認証子K_oを発生させ、この認証子K_oをICカード1に送信する。

【0058】ICカード1のCPU10は、認証子K_oを受信して鍵格納エリア14に格納された暗号鍵を用いて復号化し、OBU2に回答する。もし、鍵が正当でなかった場合（処理NG）、ICカード1は回答することができず、OBU2はセキュリティ方式Aの可能性があると処理を終了する。

【0059】仮に、ICカード1がセキュリティ方式Aであった場合は回答を返すことができない。従って、OBU2では、認証子K_oを発行し、返信データによりセキュリティ方式の選択を行うことができる。

【0060】CPU10は、鍵が正当と確認された場合、復号化した乱数を再度鍵格納エリア14に格納された暗号鍵を用いて暗号化アルゴリズム実行器15で暗号化させて認証子K_oを発生させ、この認証子K_oをOBU2へ返信する。

【0061】OBU2のCPU20は、認証子K_oを受信して鍵格納エリア24に格納された暗号鍵を用いて復号化して乱数を復元し、自己が発生した乱数と比較する。もし、乱数が一致しなかった場合（処理NG）、ICカード違いとしてICカード返却処理を行う。

【0062】CPU20は、乱数が一致した場合に上記挿入されたICカード1を正当と認証する。本発明の料金収受システムにおける実際の運用では、セキュリティ方式A、Bの2つの方式が併用される。

【0063】すなわち、OBU2は、挿入されたICカード1により、どのセキュリティ方式が適用されるかを判断する。OBU2は、ICカード1の挿入を受けて、OBU2内部の乱数発生器23により乱数を発生させ、鍵格納エリア24に格納された暗号鍵と暗号化アルゴリズム実行器25により乱数を暗号化して認証子K_oを発生させICカード1に送信し、ICカード1から回答を待つ。回答が返ってきてICカード1の正当性が認識できれば、セキュリティ方式Bとして処理を実行する。

【0064】回答が返ってこない場合は、セキュリティ方式Aと認識して、処理を続行する。仮に、偽造ICカードを挿入した場合も回答が返ってこず、セキュリティ方式Aとして処理を続行することになる。

【0065】しかし、入口車線進入後、路側システムからOBU2がデータを受けて、ICカードにデータを送信した時点である一定時間で回答が戻ってこないため、タイムアウトとしてICカード異常としてOBU2が認識することができる。偽造のICカードが偽のデータを送信した場合は、OBU2で判断できないが、出口車線でデータの送受信を行うことにより、路側システムがI

Cカード異常と認識することができる。

【0066】次に、本発明に係る均一車線のみで構成されるオープンシステムにおけるセキュリティシステムについて説明する。均一車線のみで構成されるオープンシステムでは、入口または出口の均一車線機器のみで無線による料金収受が行われるので、上述したセキュリティ方式Bで運用される。すなわち、車両が均一車線機器（料金所）進入前に、事前にICカード1がOBU2に対してデータ送信が可能な方式となる。

【0067】なお、図9で説明したセキュリティ方式Bでは、ICカードが復号化でOBU2の正当性を確認して鍵が正当でない場合にセキュリティ方式Aとしたが、オープンシステムでは、セキュリティ方式Aは有り得ないので処理NGでICカード返却とする。

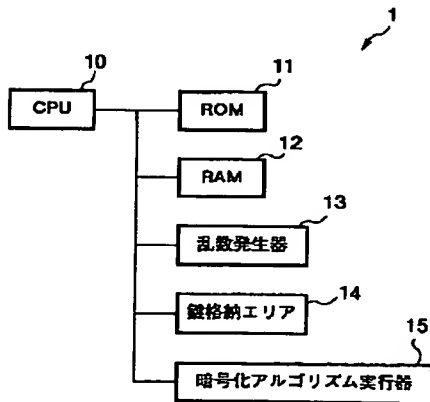
【0068】そして、OBU2は、事前にICカード1が正当と認識した際、図5で示した均一車線機器におけるブース内機器53の料金処理機50と無線によって料金収受の処理を行う。

【0069】以上説明したように上記発明の実施の形態によれば、OBUが2つセキュリティ方式を使い分けることが可能であるため、仮にセキュリティ方式Aで運用を開始した後に、セキュリティが破られた場合にも、OBUを交換せずにICカードだけを変更することにより、セキュリティ方式を切り替えることが可能になる。一方、ICカードを入れ替えることにより、2つのセキュリティ方式を切り替えることも可能である。

【0070】

【発明の効果】以上詳述したようにこの発明によれば、無線で料金の収受を行なう料金収受システムにおける無線通信回線のセキュリティの向上を図ることのできる料金収受システムと料金収受方法を提供することができる。

【図1】



【図面の簡単な説明】

【図1】この発明の料金収受システムに係るICカード1の構成を示すブロック図。

【図2】OBUの構成を示すブロック図。

【図3】クローズドシステムに用いられる入口車線機器の構成を示す図。

【図4】クローズドシステムに用いられる出口車線機器の構成を示す図。

【図5】オープンシステムに用いられる均一車線機器の構成を示す図。

【図6】通行券自動発行機の構成を示す図。

【図7】出口車線制御装置の構成を示す図。

【図8】セキュリティ方式Aの動作を説明するためのフローチャート。

【図9】セキュリティ方式Bの動作を説明するためのフローチャート。

【符号の説明】

1…ICカード

2…OBU (On Board Unit)

10、20、301、401…CPU

11、21、302、402…ROM

12、22、303、403…RAM

13、23、304、404…乱数発生器

14、24、305、405…鍵格納エリア

15、25、306、406…暗号化アルゴリズム実行器

30…通行券自動発行機

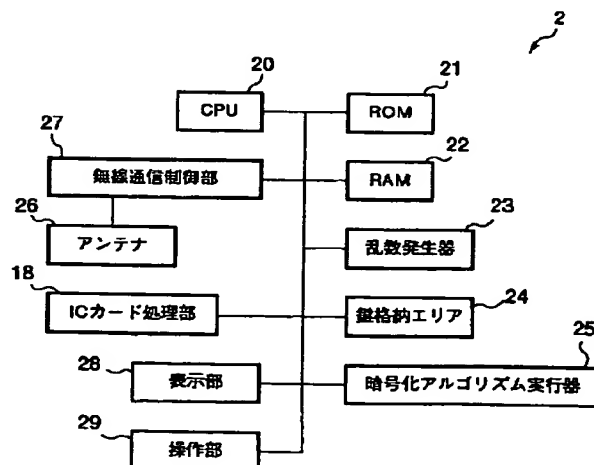
40…出口車線制御装置

43…出口ブース内機器

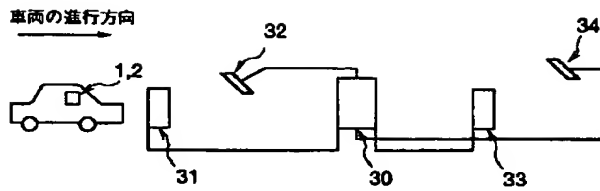
50…料金処理機

53…ブース内機器

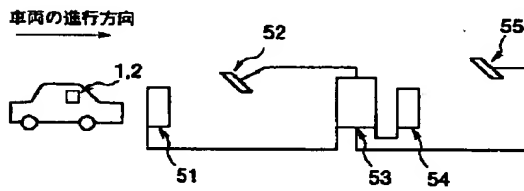
【図2】



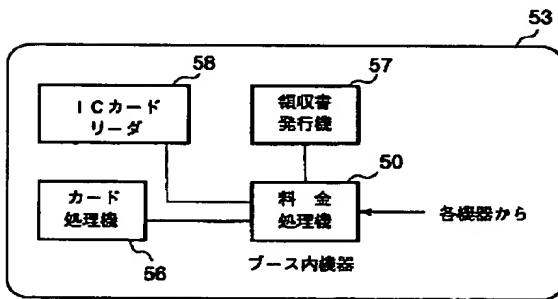
【図3】



【図5】

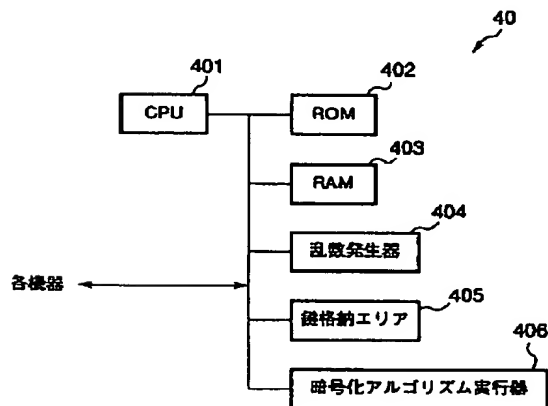


(a)

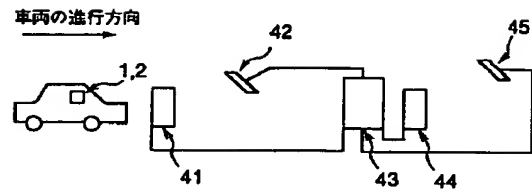


(b)

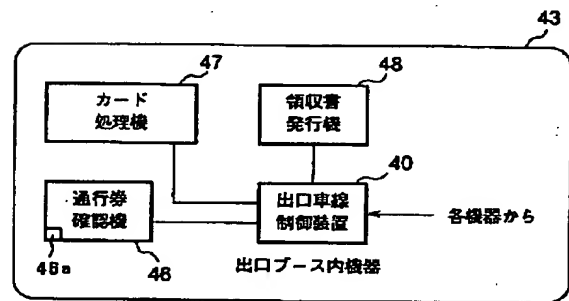
【図7】



【図4】

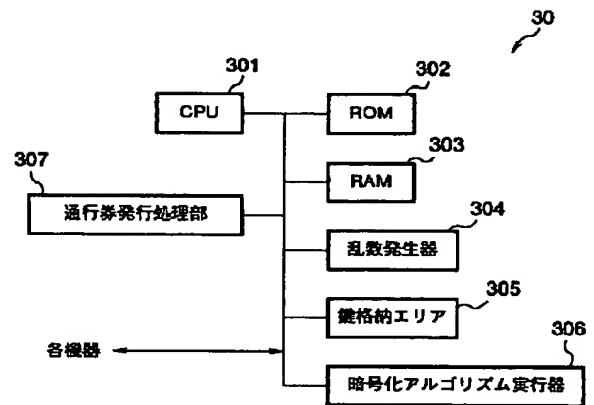


(a)

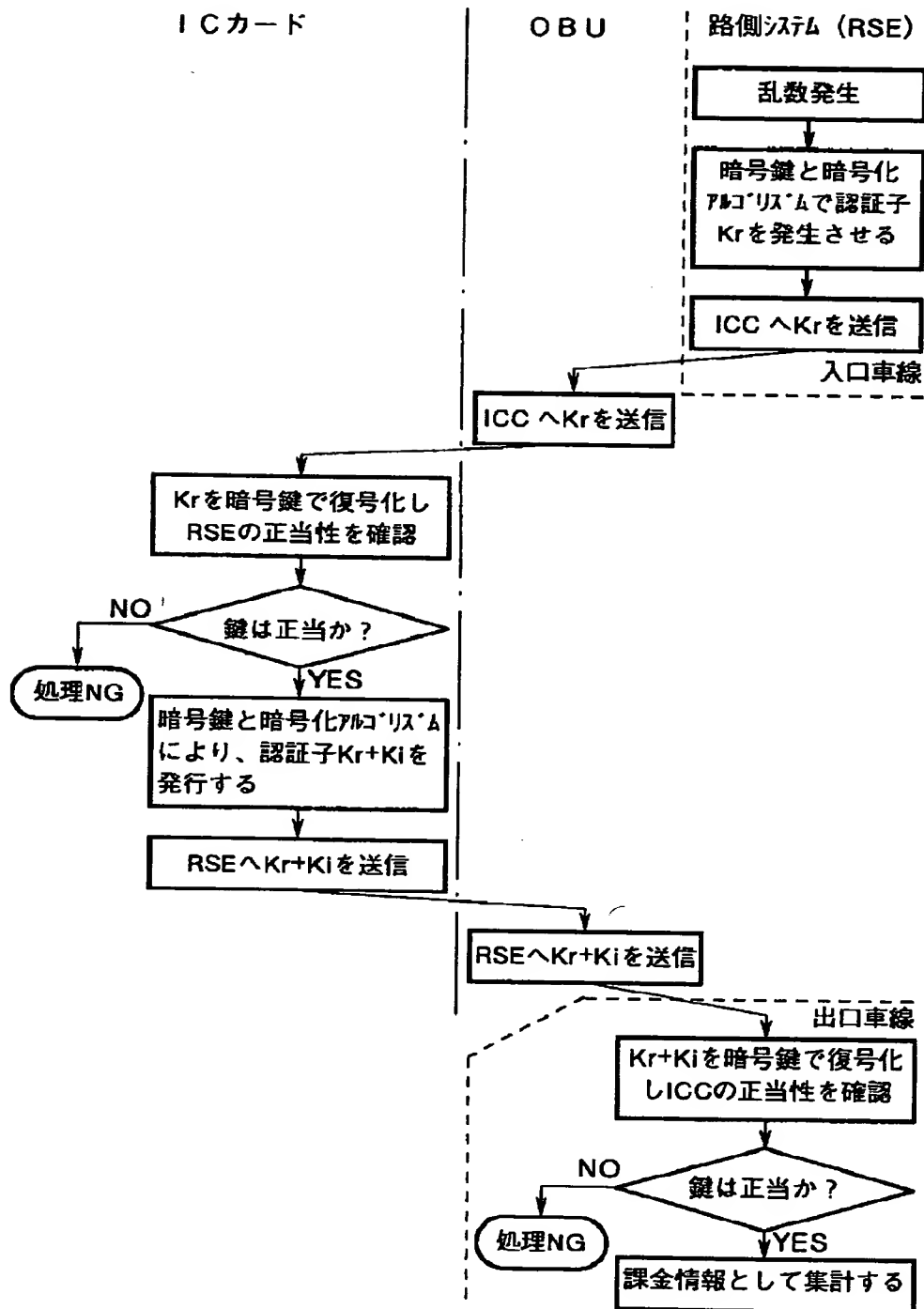


(b)

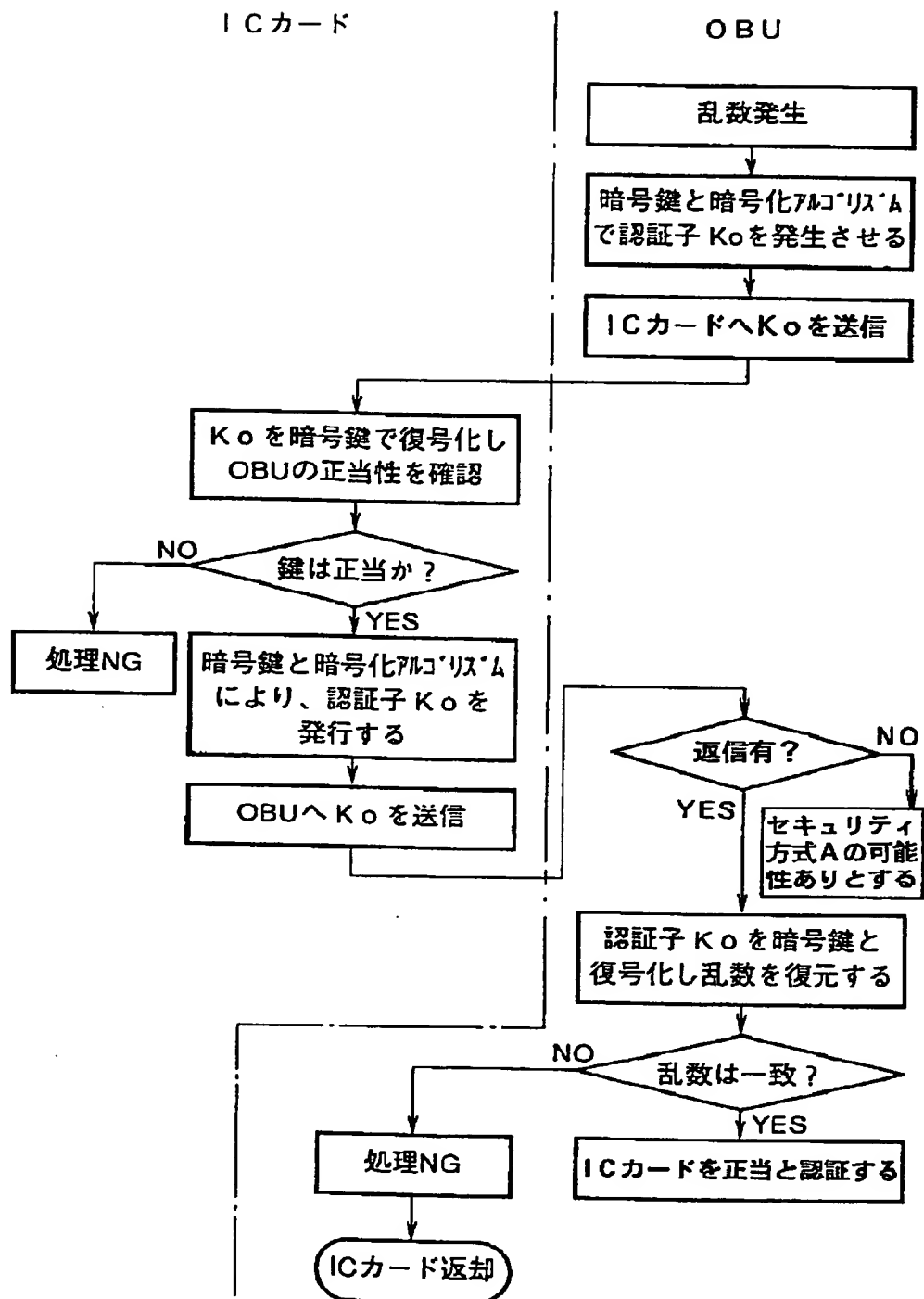
【図6】



【図8】



【図9】



(12)

特開平 10-134214

フロントページの続き

(51)Int. Cl.⁶

H 0 4 L 9/32

識別記号

F I

H 0 4 L 9/00

6 7 3 E

(72)発明者 北折 昌司

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内